Information Security Human Resource Development Program

July 8, 2011
Information Security Policy Council

Table of contents

1. Preface

As economic activities and social life have been increasingly relying on information communication technologies in recent years, information security risks have also been becoming more complex and diverse. Therefore, it is an urgent matter to establish information security that is far superior to the current practice.

In response to such changes in the social situation, the Information Security Policy Council (Chairperson: Chief Cabinet Secretary) has developed the "Information Security Strategy for Protecting the Nation" (May 11, 2010, hereinafter "Information Security Strategy") and the annual plan of information security strategy the "Information Security 2010" (July 22, 2010, hereinafter "Annual Plan") to promote general information security policies among public and private sectors.

Information security human resource development was discussed in the Information Security Policy Council "Expert Committee on Human Resources Development/Systemization of Qualifications" in 2006 and the "Expert Committee on Human Resources Development/Systemization of Qualifications Report" (January 2007, hereinafter "HR Expert Committee Report") was produced as a result to summarize the current status, issues, and future development policies of information security human resources.

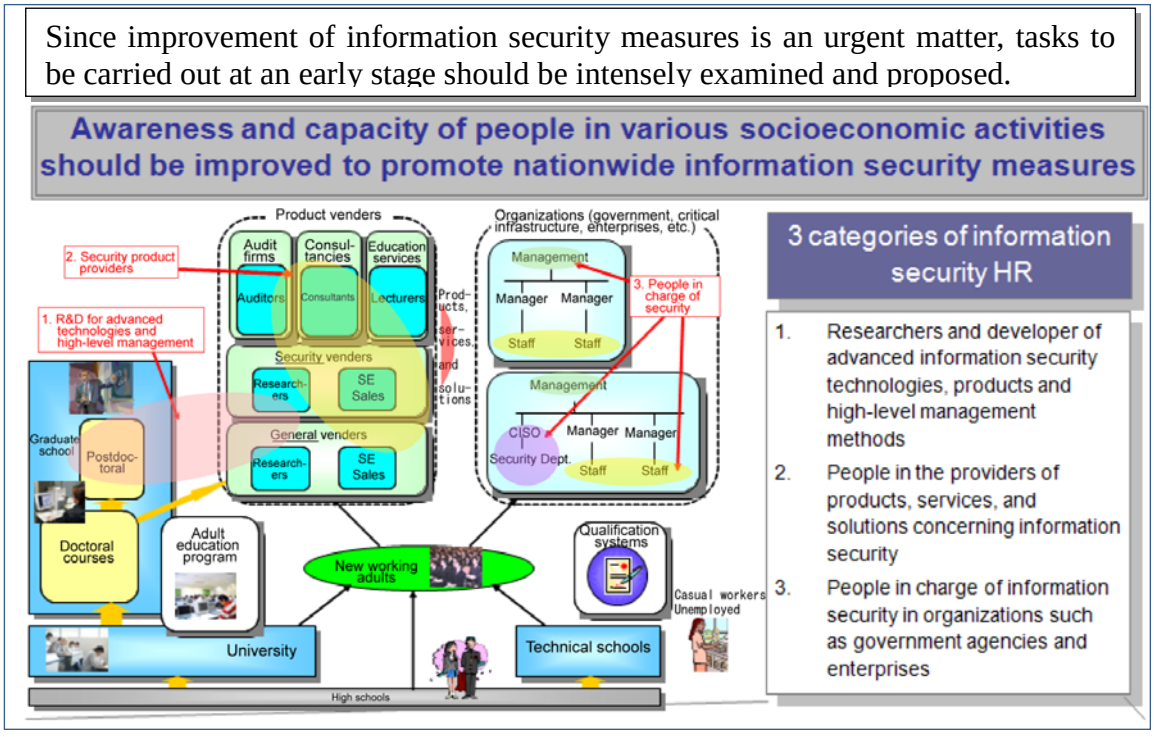

Figure 1 "HR Expert Committee Report" outline

Despite the government's efforts to enforce and promote human resource development policies based on the HU Expert Committee Report, information security risks derived from rapid changes in surrounding environments in recent years have been overwhelmingly wide-ranging. It is also hard to say that information security human resource development in organizations including that of international players has been successful.

Therefore, the "Information Security Human Resource Development Program" (hereinafter "HR Development Program") is developed to examine the future direction of the human resource development policies for various information security issues described in the Information Security Strategy, Annual Plan, and HR Expert Committee Report. This also points out areas that require more attention.

The HR Development Program assumes 3 years (2011 to 2013). Since human resource development is a medium term project, the HR Development Program contains this point of view. The HR Development Program is assessed by the "HR Expert Committee for Dissemination and Enlightenment" (tentative name) which will be described later, and the program may be revised as necessary.

Reference: Relationships between human resource development, and dissemination and enlightenment

Well balanced improvement of information security in Japan can only be achieved when advanced human resource development for high-level information communication technologies and dissemination and enlightenment policies for wide-ranging general public are both applied.

The human resource development program is aimed for information security human resource development in government agencies, enterprises, educational bodies and so on. Dissemination and enlightenment policies will be promoted based on the "Information Security Dissemination and Enlightenment Program". These two programs will be implemented to improve information security in Japan in the same time.

2. Current status and issues concerning information security human resources

While the necessity and importance of information security human resource development have increased, there are new issues and many unsolved issues. In this way, there is a gap. A structural reorganization is required to resolve such issues and establish effective and efficient human resource development.

(1) Enlarging gap

1) Shortage of human resources to deal with high-level and diverse information security threats

There is a shortage of human resources to deal with rapid changes while information security threats are complex and diverse then ever such as larger scale cyber attacks, realization of them, and emerging "new types of attacks", and security threats on cloud computing, smartphones, etc. In order to deal with such rapid changes, active and dependable information systems should be implemented and operated rather than taking a passive approach as before. Therefore, information security human resources for researching, developing, implementing, and operating such systems are vital. Also, human resources with wide information security knowledge to understand and effectively apply such high-level information security technologies are required.

2) Shortage of information security human resources in every area

Information security knowledge is needed in every area, but there is a shortage of human resources who can correspond. Information communication technologies play an important role as the social infrastructure in today's highly developed society where the scale of information utilization is increasingly expanding and the speed of information transfer is increasingly accelerating. Dependency to the information technologies is so high that socioeconomic activities and everyday life cannot be considered without them. Such a trend is deemed to continue even faster and the importance of information security technologies is increasing since they are essential for implementing and operating secure and safe information systems.

Previously information security professionals had a very restrictive nature and could be recognized as a special and separate occupation; however, awareness of information security is required in all areas in today's world.

(2) Lack of understanding among organization bosses

It is considered that bosses of organizations rarely consider information security as their strategic issues and often leave the risk management of information assets to the information system department or similar divisions in the workplace. Such attitude will only result in the situation where the intention of management remains unclear in addition to lagging application of information security measures in the workplace.

There may be lack of regulation in information security among management themselves such as information security measures are not assessed properly to assist decision-making of the management. Information security measures in organizations have often been left to the information systems personnel in the workplace as it was ridiculed as "chief clerk security". Such an approach is not sufficient to manage risks in organizations.

The mass scale information system failure immediately after the Great East Japan Earthquake eventually developed into organizations' top management crisis because of the handling error of the incident. Also, cases such as illegal access to organizations' information systems resulted in private information leakage worth tens of millions of people over dozens of countries caused international debate. Such media reports should be a wake-up call for management of organizations. They may have previously thought it was acceptable to leave information security to the personnel in the workplace; however, they must understand that mis-handling of security incidents may threaten the organization's operation and force the management to take responsibility in today's environment where organizations are strategically using information communication technologies and business operations are densely networked.

(3) Risk management vulnerabilities

The Japan Earthquake revealed risk management vulnerabilities in Japan. We must learn important lessons from the earthquake. Therefore, in addition to existing restrictive risks such as anti-virus, illegal access measures, and information leakage measures, response capability to even more inclusive information security risks must be reinforced through risk communication and risk management for a wider range of information security risks such as how to reduce business continuity risks in an ever-changing environment, etc. Consequently, it is important to develop human resources to handle information security risks in such a broad sense.

While various issues concerning the response to the earthquake have been pointed out, a number of helpful cases have also been reported such as the good use of the new media such as social networking services (SNS) and voluntary work in information communication areas. Risk response capabilities will improve with such selfless and creative action from each member.

(4) Insufficient university-industry collaboration (difference between needs of industry and seeds of educational bodies)

University-industry collaboration is desired since practical education is essential for development of information security human resources. However, it has been pointed out that there are differences in the nature of human resources educational bodies are aiming to develop and industry requires. These differences must be resolved urgently. Others also pointed out the difficulty in attaining cooperation from enterprises because the human resource development in educational bodies has no direct benefit for them.

In order to develop human resources with response capacity to risks such as business continuity, it may be effective to establish inter-faculty courses that cover security and risk management and to actively introduce internship at enterprises.

(5) Shortage of international players

As globalization is progressing worldwide in every area, the information communication industry and information security industry have gained greater mobility over national boundaries. Information security professionals in Japan are also required to be international players in such a social environment. Therefore, Japanese information security industry must aim at human resource development for international players from the early stage in order to improve international competitiveness.

Universities should actively provide internship opportunities at overseas security concerned organizations as part of their information security education.

(6) Lagging information security human resource development system in Japan

Our study of overseas international security human resource development found their various implementations. Information security human resources are developed by public and private sector collaboration, through events such as information security technology contests, and by higher education institutions' own initiatives. Meanwhile awareness of information security human resource development in Japan is not high, and the development is lagging far behind other countries despite it is a matter of strategic areas.

(7) Issues in areas

1) Developing human resources in government agencies

With regard to information security human resource development in government agencies, officers and administrators such as the chief information security officer have been appointed and the human resource development system for information security measures has been established based on the "Standards for Information Security Measures for the Central Government Computer Systems" (hereinafter "Standards") which were developed and revised by the Information Security Policy Council.

However, it takes a long time to train someone to be a highly skilled information security professional. Such staff may not be appointed to take charge of information security measures in many agencies. Also, it is difficult to build a career path for information security staff due to the personnel transfers every two or three years.

2) Developing human resources in enterprises

Almost all enterprises use the Internet[1]; however, "difficult to establish security measures", "virus threats", and "low security awareness among employees" are listed as main issues in the use of the Internet and corporate LANs. [2]

Most of enterprises which use the Internet or corporate LANs have some forms of security measures in place; however, these are normally just conventional measures such as installing anti-virus software.

OJT (On the job training) is the only means of human resource development in many enterprises without expertise to establish human resource development strategies. Planned approach is rarely taken thus opportunities of human resource development are scarce due to the recent reduction in OJT opportunities and a lack of awareness of information security human resource development.

Information communication technologies have permeated throughout corporate activities and the impact caused by the response to information security risks on corporate business is increasingly critical. Development of human resources to deal with ever more complex and diverse information security treats is desired.

3) Developing human resources in postgraduate courses

Postgraduate courses mainly carry out high-level R&D concerning information security, whereas industry requires practical information security technologies as the component technology to embed into products and services. Differences in what they pursue prevent those researchers from entering industry. Also, differences in the research subjects and human resource types discourage human resource exchange and joint research between industry and academia.

---

1 Reporting "98.8% of enterprises use the Internet" in the "Communications Usage Trend Survey in 2011" by the Ministry of Internal Affairs and Communications on May 18, 2011.

2 "Communications Usage Trend Survey in 2011" by the Ministry of Internal Affairs and Communications on May 18, 2011.
"Issues in the use of the Internet and corporate LANs (enterprises) (multiple-choice question) (end of 2010)"

4) Education in universities

Universities have important social responsibility as the base where knowledge is created and transmitted from. Information communication technologies have become vital for education and research in universities and they are required to use information safely with common recognition on information security. Information security is becoming no longer a special concept for corporate personnel and human resources for inclusive information security risks are in need; however, it is considered there is a shortage of such human resources.

The subject information security requires knowledge on various peripherals in addition to specialized knowledge in information security itself. Therefore, it is important to establish the collaboration framework and education system where students are able to gain in-depth knowledge in his own area while cooperating and liaising with specialists in other areas.

5) Education in elementary and secondary education stages

With regard to information security education in schools, the "Government Course Guidelines" revision in 1998[3] promoted information education such as active application of computers and information communication networks and the "Government Course Guidelines" revision in 2008 and 2009[4] promoted application of information communication technologies in information education and on guidance in school courses including full guidance on information ethics[5].

As the performance of mobile devices has improved, the use of Internet with these devices is rapidly spreading. This has resulted in problems such as slander and bully on the Internet, Internet crime, distribution of illegal or harmful information, and private information leakage. The importance of information security is also increasing.

It is becoming increasingly important to approach information ethics education on thorough understanding of both glory and danger of the Internet. The basic concept and attitude such as basic rules and manners in information society and the safe use of information communication technologies should be taught through all subjects in addition to the moral lessons.

6) Leadership of teachers

Each teacher should understand that they should improve their abilities to teach how to use information communication technologies. They should actively take

---

[3] The "Government Course Guidelines" for elementary and junior high schools were revised in December 1998 and the "Government Course Guidelines" for high schools were revised in March 1999. Specifically, "Information and computers" was made the mandatory item in the manual training and domestic science subjects (technical subjects) in junior high schools and the new subject "Information" was made mandatory and another technical subject "Information" was also introduced in high schools.

[4] The "New Government Course Guidelines" for elementary and junior high schools were revised in March 2008 and the "New Government Course Guidelines" for high schools and special support schools were revised in March 2009.

[5] "Information ethics" is "the basic concept and attitude for appropriate activities in the information society"

advantage of the school's internal seminars as well as carry out their own study. The education board should also be involved in schools' seminars and enhance their own seminars. Public schools are equipped with nearly one computer per teacher at the end of March 2010. Therefore, information security has become an unavoidable issue in today's computerized school operations.

Teachers' knowledge and teaching ability of information security may vary, but teachers may not have enough opportunities to learn about information security due to the pressure of education tasks.

3. Basic approach

The following describes the government's basic approach to promote human resource development based on the environmental changes of information security and the past approach and issues concerning information security human resources development.

Basic concept of information security human resource development

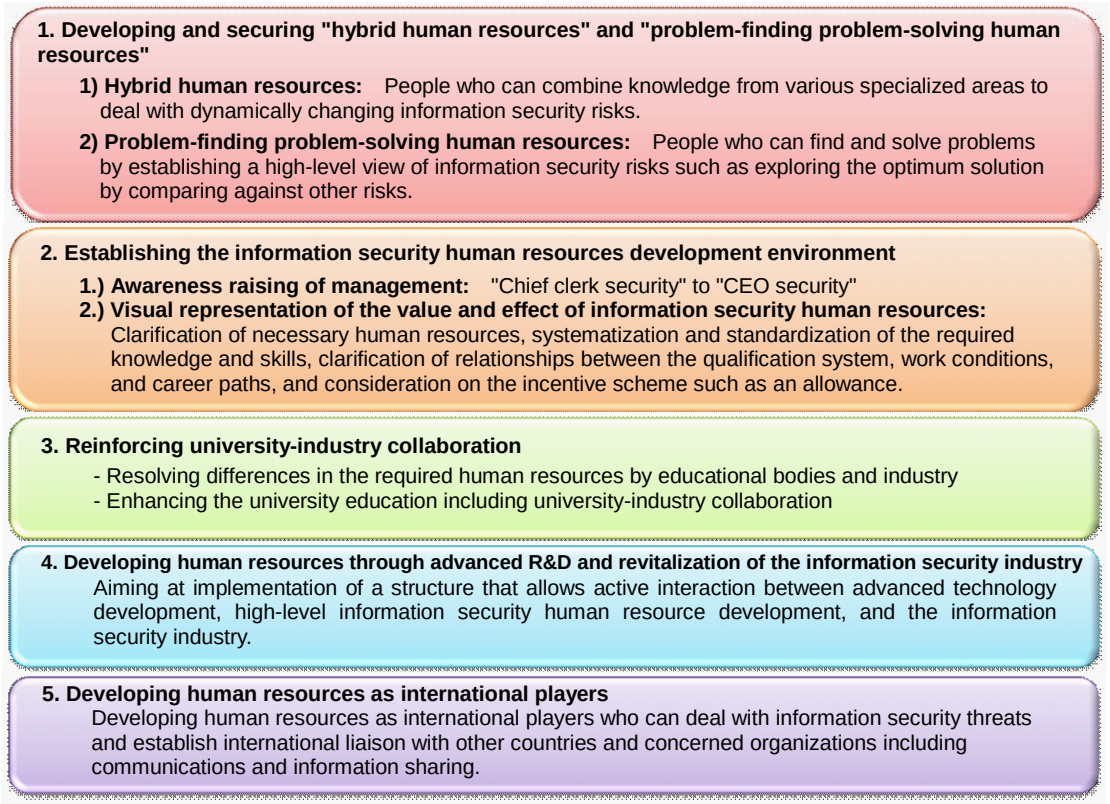

Figure 2 Basic concept of information security human resource development (outline)

(1) Developing and securing "hybrid human resources" and "problem-finding problem-solving human resources"

The area of information security human resources is closely related to other areas such as mathematics, computer science, and communications engineering for the technical aspect, and economics, law, accounting, sociology, and group psychology from the management aspect. Also, information security measures cannot be implemented just technically from the information systems' viewpoint since they are also closely related to audit and legal operations in enterprises. Therefore, information security human resources are required to possess management and risk management expertise in addition to technical expertise concerning information systems and information security. Since technological innovations occur frequently in information communication technologies compared to other areas, information security specialists should be able to understand the future technical trends and their impact in the event

of paradigm shifts, and to deal with dynamically changing risks of increasingly complex and diverse information security threats. Therefore, information security specialists need to be the humanities and sciences "hybrid" type who can combine expertise of various areas rather than being a specialist of one area.

Information security risks cannot be dealt with a single measure but a combination of various measures. Also, as the situation changes dynamically, the acceptable risk level changes significantly thus information security specialists should be able to take the optimum risk response even to a sudden violent change of the situation. Also, a measure to a certain risk may create another risk. Therefore the specialists need to be the "problem-finding problem-solving" type who are able to see the whole picture of relationships between ever-changing information security risks and find the optimum solution.

The Great East Japan Earthquake made us realize the importance of risk communications and risk management, and nationwide reinforcement of risk response abilities is desired. Since information security must assume the risks that change constantly and globally, the knowledge we can acquire through human resource development of this area can be applied to develop human resources to deal with mass scale disasters.

Previously technical abilities are preferred for information security human resources. However, developing "hybrid" and "problem-finding problem-solving" human resources is important in the environments where enterprises are relying heavily on information communication technologies both for business management and strategies while information security is also positioned as the infrastructure technology for information communication technologies.

(2) Establishing the information security human resources development environment

1) Awareness raising of management

- "Chief clerk security" to "CEO security"[6] -

Management must change their attitude and stop leaving information security measures to information systems personnel in the workplace ("chief clerk security").

While management is aware that they are responsible for the organization's risk management, they do not normally recognize information security risk measures in the same way. However, critical parts of corporate activities are relying on information communication technologies and their risk measures are for information security, thus information security measures are crucial issue for the business. Establishing and maintaining information security is vital for the corporate management in order to protect intellectual assets such as technical information, remain highly competitive, and grow the enterprise. Since information security is risk measures, it optimizes organization-wide cost effectiveness and there is nothing different from other issues that require

6 Koichiro Hayashi "Chief Clerk Security to CEO Security: Japanese Management and Information Security (In Japanese)" available at :http://www.iisec.ac.jp/proc/vol0002/iisec_proc_002_p001.pdf (last visited July 2011)

management decisions. Finally information security measures must conform and integrated with the governance of overall business and responsibilities (internal control, compliance, quality management, environmental adaptation, organization's social responsibilities).

The above leads to the need of "CEO security" for information security measures in today's changeable situation. No need to mention the recent mass scale information system failure in private sectors and large scale private information leakages in the chapter describing issues concerning information security.

In order to promote information security measures, all employees including management should share the same awareness of risk management and establish an environment that can sustain the morals and motivation.

Also, it is important to develop human resource for more active communications between employees and management for smooth governance concerning information security.

"CEO security" will probably contribute towards solving existing problems in information security human resource development in enterprises such as i) Unrelated to the working conditions, and ii) Difficult to improve work satisfaction and motivation. This may improve the social status of people who work for information security and will make it an attractive occupation.

2) Visual representation of the value and effect of information security human resources

It is difficult to secure human resources in the environment of decreasing birthrate and aging population and the working condition is harsh. Industry and enterprises need to clarify the required information security human resources and visually represent the effects. The required knowledge and skills are neither systematized nor standardized in many enterprises and as a result the skills are retained on individual basis.

The review of the qualification system and training program should continue as it was pointed out in the HR Expert Committee in 2007. It is important to clarify the relationships between the qualification system, work conditions, and career paths in order to secure information security human resources. Also, considerations should be given to the incentive scheme such as an allowance (information security personnel assessment, preferential treatment system, etc.).

(3) Reinforcement of university-industry collaboration

It has been pointed out that there are differences in the nature of human resources educational bodies are aiming to develop and industry requires. These differences must be resolved urgently. University education including the fruit of university-industry collaboration has been criticized to lack practical information security education. In order to solve these issues, the Ministry of Education, Culture, Sports, Science and Technology took initiative in the "Leading IT Expert Development Promotion Program" in 2006. In response to that, the "ISS Square"

(Institute of Information Security, Chuo University, Tokyo University) and "IT Keys" (Nara Institute of Science and Technology, Chuo University, Tokyo University, Japan Advanced Institute of Science and Technology, Osaka University, Kyoto University) were selected as the programs to develop human resources on the world highest level in information security by combining study and business practice beyond boundaries of universities and between universities and industry in 2007.

University name	Project name	Project outline
- Nara Institute of Science and Technology - Kyoto University - Osaka University - Japan Advanced Institute of Science and Technology	IT Keys Information security engineer and manager education to reduce social IT risks	The objective is to develop human resources who can take initiative in planning and applying information security measures in both public and private sectors. A training course is established jointly between four graduate schools of information technology mainly in the Kansai area. The course systematically teaches management methods of organizations and general risk measure techniques for information systems. The course actively accepts working adults and train practical specialists through lectures given by lecturers invited from organizations and enterprises, and practical exercises.
- Institute of Information Security - Tokyo University - Chuo University	ISS Square Advanced information security human resource education program by combined research and business practice	A university-industry collaboration program to combine research and business practice by Institute of Information Security, Chuo University, Tokyo University, NII, NICT, and eight more enterprises to train high-level security specialists. The program develops human resources for leaders with wide-ranging knowledge and highly practical abilities in information security through lectures and exercises covering an ample choice of subjects. The program also develops human resources for high-level R&D with problem-solving abilities through advanced and open research activities aided by the university-industry collaboration.

Figure 3 Leading IT Specialist Development Promotion Program (selected programs in 2007)
""Leading IT Specialist Development Promotion Program " selection status" by Ministry of Education, Culture, Sports, Science and Technology, September 2007

The budget measure finished in 2010; however, this program was the model case to develop high-level information security human resources in Japan. Since human resource development is a medium to long term project, this should not be recognized as a one-off project but the beginning of the continuing effort to develop information security human resources on the world highest level. This project is the best practice that has come out of university-industry collaboration and we hope the budget will be provided in some way.

(4) Developing human resources through advanced R&D and revitalization of the information security industry

As it is pointed out in the "Information Security Research and Development Strategy" we should lead the world in research and development concerning "New dependability" to combat information security issues in cloud computing and smartphones and complex and diverse threats from new types of attacks.

High-level information security human resources are required to carry out such research and development. We will be able to contribute towards the international competitiveness of Japanese information communication and information security industries and their global development if the research and development produce pioneering results. Therefore, we should take an active approach to implement a structure that allows active interaction between advanced technology development,

high-level information security human resource development, and the information security industry.

(5) Developing human resources as international players

Globalization of Japanese enterprises is advanced and many enterprises have entered into overseas markets. Information communication networks act as the nervous system between those enterprises and their overseas branches, and the needs for information security is increasing. International liaison such as information sharing with concerned organizations is essential for accurately dealing with cyber attacks and computer viruses since they have no international boundaries. The status of information security technologies should be understood from the global viewpoint since they also have no international boundaries. It is a matter of urgency to develop information security human resources as international players since such trend will only accelerate.

4. Specific efforts

(1) Establishing the HR Expert Committee for Dissemination and Enlightenment (tentative name)

The "Information Security Policy Council" specializes development and assignment of information security human resources. In order to clarify its "control tower" function, the "HR Expert Committee for Dissemination and Enlightenment" (tentative name) will be established to advice and assess the dissemination and enlightenment, and human resource development policies for information security. The "HR Expert Committee for Dissemination and Enlightenment" (tentative name) will advice and assess as follows.

i) Review if the specific approach of the human resource development program is contributing towards development of the "hybrid" and "problem-finding problem-solving" types as described in "3. Basic approach".

ii) Monitor the progress of human resource development programs in government agencies, enterprises, and educational bodies. Discuss the cause and solution and provide advice as necessary if the progress is not satisfactory.

iii) Review the effect of various qualification systems and educational programs as many as possible and provide advice for improvement as necessary.

iv) Review the relationships between qualification systems, career paths, and working conditions as necessary if possible.

v) Advice on policy reviews and new policies based on the environmental changes in information security.

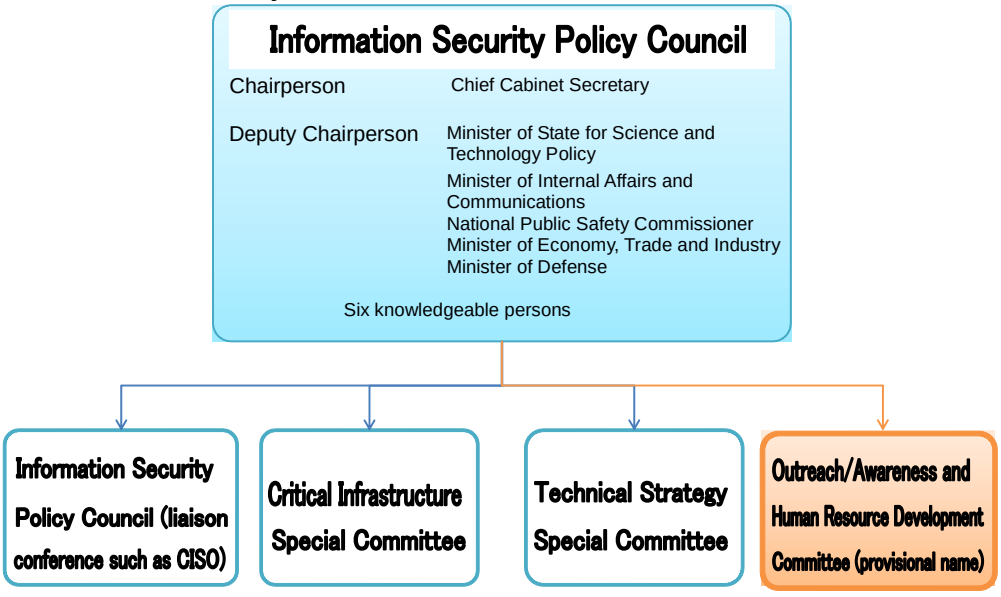

Figure 4 Positioning of the "HR Expert Committee for Dissemination and Enlightenment" (tentative name)

(2) Developing advanced information security researchers and specialists

In order to improve the nation-wide information security level and reinforce international competitiveness of the information security area, we must develop a number of advanced information security researchers and specialists who are able to lead the world. This issue is closely related to enhancement of university education and the direction of R&D in various research organizations. Human resources for advanced researchers and specialists should be developed with strategic promotion of the newly developed "Information Security Research and Development Strategy" in cooperation with the Science and Technology Basic Plan since the research and development involve the internationally acceptable Japanese technologies and university technologies which may influence products and business in industries.

Also, public and private sectors should collaborate on promotion of the research and development to develop new technologies to solve information security issues in cloud computing, smartphones, IPv6, and SNS, and contribute towards development of high-level information security human resources though implementation of coordinated human resource network using a cyber security research testbed.

(3) Developing human resources in government agencies

Government agencies have decided the Information Security Standards in the Information Security Policy Council as the new basic policies to cope with changes in awareness, technologies, and environments of today's information security, and to help understanding information security measures by the chief information security officer.

The human resource development policies should be promoted based on these Information Security Standards among legal employees. Specifically, enhancement of standardized education programs and material templates, and drills concerning targeted e-mail attacks to improve information security knowledge of legal employees.

(4) Developing human resources in enterprises

1) Awareness raising of management

Fundamental reform must take place in enterprises to turn "chief clerk security" to "CEO security" where management of enterprises take initiative in information security. In order to assist them it will be useful to establish a system where they can share success and failure cases in information security measures in business operations including overseas examples. Also, discussion should be held on information security measures and human resource development policies from the organizational risk management viewpoint in places where management of enterprises may meet.

2) Establishing the organization-wide human resource development environment

Development and permeation of human resource development plans that define information security human resource development policies and clear career paths should be promoted in enterprises. Human resource development in enterprises

will be promoted by clarifying relationships between i) Required human resource definition, ii) Qualification systems and education programs, iii) Career paths, iv) Work conditions (assessment system).

The person who makes the human resource development plan should examine the type of human resources required in his organization and refer to required capabilities and education programs. Also, it is important to clarify the type of the information security human resources required in each organization within the enterprise, and systematize and standardize the required knowledge and skills. Information security requirements should be reviewed in parallel with the business reform and system reform and the human resources who can carry out such requirements should be developed.

It is effective to collect, analyze, and share best practice concerning information security human resource development plans internally and externally. Also, it is helpful to introduce a professional system to grant working conditions according to a certain assessment system for human resource development. It is needless to say that the human resource development plan should be reviewed whenever a change occurs in the information security environment and organizational strategies.

It is also effective to introduce recurrent education where working adults re-learn in high-level educational organizations to obtain systematic knowledge and to avoid the information security skills remaining as individual's possession.

3) Appointing CIO and CISO

CIO [7] and CISO [8] have authority to make final decisions concerning information security. They understand the overall status of information risks in the organization, determine the acceptable risk levels, procure and assign resources for information security measures, monitor the information security management status, and instruct improvements. Issues concerning information security may span over many business areas and often cause inconvenience or affect efficiency of business. It is important to position CIO and CISO properly in an organization for strategy development, decision making, and execution concerning information security across divisions from the organization-wide optimization viewpoint in increasingly complex corporate management.

Considering information security threats will be increasingly globalized, sophisticated, and complex, it may be a good idea to look into systems such as "information security insurance" in private sectors.

4) Critical infrastructure providers

Critical infrastructure providers should proactively develop human resources with high-level information security knowledge though cross-sectional drills and

7 "CIO" is the abbreviation of Chief Information Officer and is the person who has the ultimate responsibility in implementation and operations of information communication technologies of the enterprise and is in charge of planning and executing IT strategies according to the enterprise's management principle.

8 "CISO" is the abbreviation of Chief Information Security Officer and is in charge of planning and executing information security strategies according to the enterprise's management principle.

seminars in order to reinforce the information security infrastructure and share the status information among them.

5) Small and medium-sized enterprises

Events such as "information security leader seminar for small to medium-sized enterprises" will be held to attain information security in small to medium-sized enterprises.

(5) Developing human resources in educational bodies

It is desirable that educational bodies also focus on development and attainment of "hybrid" and "problem-finding problem-solving" types of human resources. In addition to inter-faculty, inter-university, and university-industry collaboration, it will be advantageous to deploy methods which encourage students to find and solve problems rather than being restricted within the knowledge passing method.

1) Enhancing university education

"ISS Square" and "IT Keys" aim at development of the best information security human resources in the world and they are extremely valuable in many aspects such as university-industry collaboration, inter-university collaboration, high-level information security human resource development, and international competitiveness. It is important to correctly assess and continuously develop such success cases. Human resources who are highly specialized in information security should be developed in graduate schools. Also adult education program should be enhanced in liaison with industries by establishing information security risk management courses where humanities and sciences are both integrated.

It is desirable to establish a systematic and balanced curriculum of theoretical and practical education of economics, management, information communication engineering, information security engineering, and enhance education contents with consideration to various needs from students from different backgrounds such as new graduates and working adults based on information security in a broad sense including risk management in enterprise/organization management, in order to develop high-level specialists who can understand management and technologies.

2) Enhancing information security education in universities

It is important to have awareness of information security when students go out in the world. Universities may take initiative in providing more opportunities to learn information security in their core and general education. Therefore, universities should be encouraged to provide minimum necessary education for information security though subjects such as information ethics. Also it may be helpful to enhance teaching materials and tools, and to establish an environment where students can widely learn the concept of risk management, intellectual properties, privacy, etc.

Teaching structures and materials for faculties concerning information processing should be enhanced by inter-university liaison to cover sophisticated and wide-ranging information security threats. Also, it is effective to provide opportunities for students to participate in overseas academic meetings and internships to develop information security human resources as international players, to improve mutual understanding with other countries, and to form human networks.

3) Enhancing practical hands-on education

Information security often require hands-on experience and its education should be practical rather than simply attaining the knowledge. Increasing hands-on exercises and inviting lecturers from enterprises will be useful and will also improve university-industry collaboration.

4) Enhancing information security education in elementary and secondary education

Information security education for elementary and secondary education according to pupils' each development stage though a common subject "Information" and others has been enhanced by 2008 and 2009 revisions of "Government Course Guidelines" It is important to provide education in line with the information security trends.

5) Enhancing information security seminars for teachers

A seminar system should be established for teachers to learn information security. Also, the latest trends of information security should be notified to them though meetings such as the information education staff meeting to ensure that they can provide appropriate education to students.

(6) Reinforcing university-industry and public-private collaboration

1) Promoting education by university-industry collaboration

Differences in the needs of industry and educational bodies should be resolved by mutually clarifying and understanding advantages of each other's argument. Educational bodies should promote and continue education to develop practical human resources who can work in the global market with the cooperation of enterprises. The approach taken by "ISS Square" and "IT Keys" can be used as the reference. Also it will be effective to actively take advantage of internships in domestic and overseas enterprises.

2) Promoting collaboration for practical education

University-industry collaboration should be reinforced to establish practical information security education, such as jointly designing education curriculum, inviting lecturers from enterprises, and encouraging interaction employees in

enterprises, university teachers, and students. Personnel interaction between the information security industry and other industries may also be encouraged.

3) Taking advantage of information security contests

Approaches such as making a public recognition of individuals' or enterprises' exceptional contribution towards information security, or awarding a grant to the winner of information security contests can be seen in Japan and overseas. Such incentive programs and nation-wide information security contests should be examined to secure advanced information security human resources and develop international players.

4) Promoting work experience opportunities in government agencies

Government agencies with science graduate executive officers will be encouraged to increase the internship opportunities in information security concerned departments to provide work experience for students who are interested in information security.

(7) Reinforcement of international alliances

International cooperation is essential in information security policies since information is freely moving beyond international boundaries today. It is important to liaise with other countries while reinforcing international competitiveness when the information communication infrastructure for business environments and economic activities is rapidly globalizing.

The National Information Security Center has been reinforcing the international collaboration especially with ASEAN countries in various areas though the liaison framework since 2009. Efforts for Information security human resource development in ASEAN materialized as the "Japan and ASEAN Information Security Seminar" and "Japan and ASEAN Government Network Security Workshop" in 2010, and will continue to develop.

Information security human resource development is also promoted in European and countries and the U.S.A. Various types of activities are taking place such as education programs in higher educational bodies and technical contests. It is desirable to share best practice and study the specific collaboration areas without limiting our activities within Japan in order to develop international players.

Measures taken by one country are not effective for threats beyond international boundaries and internationally coordinated information security measures are required. Therefore, human resource development though international liaison is important for cases such as cyber attacks.